Dkt. 61002

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims of the application:

Claim 1 (Currently Amended) A method for mutual authentication of components in a network using a challenge-response method to authenticate a terminal with the network, comprising the steps of:

requesting at least one data pair including a first random number (Challenge 1) and a first response (Response 1) from an authentication center using a request from the network;

passing the first random number (Challenge 1) to the terminal which ~~uses~~ calculates the first response (Response 1) based upon an internally stored key and the first random number ~~to calculate the first response (Response 1)~~ (Challenge 1);

sending the calculated first response (Response 1) to the network; and

~~sending a second random number (Challenge 2) from the terminal to the network; and~~

responding to ~~the~~ a second random number with a second response (Response 2) calculated in the authentication center, the response performed by the network, wherein

the first response (Response 1) sent from the terminal to the network is also used as the second random number (Challenge 2), whereby the network has previously requested the second response (Response 2) from the authentication

center together with the first random number (Challenge 1) and the first response (Response 1) as a triplet data set (Challenge 1/Response 1/Response 2).

Claim 2 (Previously Presented) The method as claimed in claim 1, wherein the network interprets the calculated first response (Response 1) sent back from the terminal as the second random number (Challenge 2).

Claim 3 (Previously Presented) The method as claimed in claim 1, wherein the first random number (Challenge 1) and the second response (Response 2) are transmitted from the network to the terminal in succession.

Claim 4 (Previously Presented) The method as claimed in claim 1, wherein a data pair (Challenge 1/Response 2) is transmitted from the network to the terminal simultaneously in the form of a single data set.

Claim 5 (Previously Presented) The method as claimed in claim 1, wherein the network requests data sets from the authentication center in the form of triplet data sets (Challenge 1/Response 1/Response 2).

Claim 6 (Previously Presented) The method as claimed in claim 5, wherein a plurality of triplet data sets are supplied from the authentication center as a stockpile to reduce a request frequency.

Claim 7 (Previously Presented) The method as claimed in claim 1, wherein to use the first response (Response 1) of the terminal as the second random number (Challenge 2), a shorter length of the first response (Response 1) is filled out to make up a greater length of the second random number (Challenge 2).

Claim 8 (Previously Presented) The method as claimed in claim 7, wherein

the filling-out is performed on a subscriber-specific basis; and

the complete length of the first response (Response 1) is shortened before transmission to an other station.

Claim 9 (Previously Presented) The method as claimed in claim 8, wherein the first response (Response 1) is filled out with defined bits from the key to make up the length of the second random number (Challenge 2).

Claim 10 (Previously Presented) The method as claimed in claim 8, wherein the second random number (Challenge) corresponds to the first response (Response 1) before it was shortened.

Claim 11 (Previously Presented) The method as claimed in claim 1, wherein the network is a GSM network.

Claim 12 (Previously Presented) The method as claimed in claim 1, wherein the network is a wire-based network.

Claim 13 (Previously Presented) The method as claimed in claim 12, wherein components in the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 14 (Previously Presented) The method as claimed in claim 1, wherein the authentication center calculates the triplet data sets requested by the network and transmits the calculated triplet data sets to the network off-line and independently of time, on request by the network, and before ~~the~~ data interchange between the network and the terminal.